CLAIMS

What is claimed is:

1. A computer-implemented method for controlling access by a plurality of client applications to file data in a distributed file system including a distributed file system interface coupled to the client applications and a storage server and a meta-data server coupled to the distributed file system interface, comprising:

receiving at the meta-data server an open-file request, the open-file request specifying a name of a first file, wherein the first file includes a first set of blocks;

creating a security object at the meta-data server in response to the open-file request;

generating an encryption key at the meta-data server and the storage server and storing the encryption key in the security object;

encrypting a list that identifies the first set of blocks, whereby an encrypted block list is formed;

adding the encrypted block list to the security object; and

transmitting the security object to the distributed file interface.

2. The method of claim 1, further comprising:

transmitting a file access request and security object from the distributed file system interface to the storage server in response to a file access request from a client application, the file access request including an operation code and a reference to selected data of a file;

decrypting the block list at the storage server in response to the file access request;

providing access to the selected data in accordance with the operation code upon successful decryption of the block list.

3. The method of claim 2, further comprising:

encrypting file data at the distributed file interface for file write operations using the encryption key in the security object; and

decrypting file data at the distributed file interface for file read operations using the encryption key in the security object.

4. The method of claim 3, further comprising:

generating a partial encryption key at the meta-data server and storing the partial encryption key in the security object;

transmitting the security object to the storage server; and

completing generation of the encryption key at the storage server using the partial encryption key and storing a complete encryption key in the security object; and

returning the security object with the complete encryption key to the meta-data server.

5. The method of claim 4, further comprising:

transmitting a close file request, along with the security object, from the distributed file system interface to the meta-data server, the close file request specifying the name of the first file;

removing the encrypted block list of the first file from the security object.

6. The method of claim 5, further comprising returning the security object from the meta-data server to the distributed file system interface after removing the block list.

7. The method of claim 6, further comprising deleting the security object if there are no block lists in the security object after processing a close file request.

8. The method of claim 1, further comprising:

encrypting file data at the distributed file interface for file write operations using the encryption key in the security object; and

decrypting file data at the distributed file interface for file read operations using the encryption key in the security object.

9. The method of claim 1, further comprising:

generating a partial encryption key at the meta-data server and storing the partial encryption key in the security object;

transmitting the security object to the storage server; and

completing generation of the encryption key at the storage server using the partial encryption key and storing a complete encryption key in the security object; and

returning the security object with the complete encryption key to the meta-data server.

10. The method of claim 1, further comprising:

transmitting a close file request, along with the security object, from the distributed file system interface to the meta-data server, the close file request specifying the name of the first file;

removing the encrypted block list of the first file from the security object.

11. The method of claim 10, further comprising returning the security object from the meta-data server to the distributed file system interface after removing the block list.

12. The method of claim 11, further comprising deleting the security object if there are no block lists in the security object after processing a close file request.

13. An apparatus for controlling access by a plurality of client applications to file data in a distributed file system including a distributed file system interface coupled to the client applications and a storage server and a meta-data server coupled to the distributed file system interface, comprising:

means for receiving at the meta-data server an open-file request, the open-file request specifying a name of a first file, wherein the first file includes a first set of blocks;

means for creating a security object at the meta-data server in response to the open-file request;

means for generating an encryption key at the meta-data server and the storage server and storing the encryption key in the security object;

means for encrypting a list that identifies the first set of blocks, whereby an encrypted block list is formed;

means for adding the encrypted block list to the security object; and

means for transmitting the security object to the distributed file interface.

14. A system for controlling access by a plurality of client applications to file data in a distributed file system, comprising:

a distributed file system interface coupled to the client applications, the interface configured to transmit open file requests to a meta-data server and file access requests to a block storage server;

the meta-data server coupled to the distributed file system interface and to the block storage server, the meta-data server configured to generate a partial encryption key, store the partial encryption key in a security object, transmit the security object to the block storage server for completion of the encryption key, encrypt a list of blocks in a file as an encrypted block list, and return the security object with the encrypted block list to the distributed file system interface; and

the block storage server coupled to the distributed file system interface, the block storage server configured to generate a complete encryption key from the partial encryption key in the security object, and return the security object with the complete encryption key to the meta-data server.

15. The system of claim 14, wherein:

the distributed file system interface is further configured to transmit a file access request and the security object to the block storage server in response to a file access request from a client application, the file access request including an operation code and a reference to selected data of a file; and

the storage server is further configured to decrypt the encrypted block list in response to the file access request and provide access to the selected data in accordance with the operation code upon successful decryption of the block list.

16. The system of claim 14, wherein:

the distributed file system interface is further configured to encrypt file data for file write operations using the encryption key in the security object decrypt file data for file read operations using the encryption key in the security object.